UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,570	03/10/2005	Markus Bockes	WACHP006	7328

25920 7590 04/29/2008

MARTINE PENILLA & GENCARELLA, LLP
710 LAKEWAY DRIVE
SUITE 200
SUNNYVALE, CA 94085

EXAMINER	
PACHURA, REBECCA L	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
04/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/527,570	BOCKES ET AL.	
	Examiner	Art Unit	
	Rebecca L. Pachura	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 14-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 14-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/10/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1 and 14-34 are presented for examination.**

The claims and only the claims form the metes and bounds of the invention. "Office personnel are to give claims their broadest reasonable interpretation in light of the supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim are not read into the claim. In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969)" (MPEP p 2100-8, c 2, l 45-48; p 2100-9, c 1, l 1-4). The Examiner has full latitude to interpret each claim in the broadest reasonable sense. The Examiner will reference prior art using terminology familiar to one of ordinary skill in the art. Such an approach is broad in concept and can be either explicit or implicit in meaning.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 07/10/2006 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Preliminary Amendment

3. The preliminary amendment to the claims submitted on 03/10/2005 is duly noted. The cancellation of claims 2-13 submitted on 03/10/2005 is duly noted. The preliminary amendment to the disclosure submitted on 03/10/2005 is duly noted.

Priority

4. The claim for foreign priority from #10250810.0 filed on October 10, 2002 and from #10242061.0 filed on September 11, 2002 are duly noted.

Specification

5. The abstract of the disclosure is objected to because there are inappropriate numbers included in the paragraph and (Fig. 2) is printed on the bottom. Correction is required. See MPEP § 608.01(b).

Claim Objections

6. Claims 14-26, 28, 29, 31, 33, and 34 are objected to because of the following informalities: Claims 14-26, 28, 29, 31, 33, and 34 all begin with *"A"* they should begin with *"The"*. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. **Claims 17 and 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.**

Claim 17 recites the limitation "*the safeguard value*" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 25 recites the limitation "*the error freedom*" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. **Claims 1, 14-20, and 26-34 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.** Claims 1, 14-20, and 26-34 in the preamble recite *"protected execution of a cryptographic calculation"* this algorithm has no result in the limitations of the claim. In view of the below sited MPEP section the claim is non-statutory because it is nonfunctional descriptive material per se. Claims 30 and 31 recite *"a computer program product which has program commands to cause a processor to execute"* a computer program product is clearly software that must be embodied in something such as a storage device, a CD or a DVD, flash memory, etc. In view of the below sited MPEP section the claim is non-statutory because it is functional descriptive material per se.

> **MPEP 2106.01 [R-5]**
> Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) "Nonfunctional descriptive material" includes but is not limited to music, literary works, and a compilation or mere arrangement of data.
>
> Both types of "descriptive material" are nonstatutory when claimed as descriptive material per se, 33 F.3d at 1360, 31 USPQ2d at 1759.

Claim Rejections - 35 USC § 102

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. **Claims 1, 14, 15, 19, 20, 27, 30, 32, and 33 are rejected under 35 U.S.C. 102(b) as being anticipated by WO 0161918 (US 20030159036) (Walmsley) (Applicant's IDS).**

As to claim 1, Walmsley discloses (Currently amended) a method for protected execution of a cryptographic calculation, in which a key ~~(12)~~ with at least two key parameters is drawn on, wherein an integrity check ~~(30, 34, 40, 54)~~ of the key ~~(12)~~ is performed (Walmsley page 36, paragraphs 0933-0945, page 14, paragraphs 0352-0354) ~~in the method~~, in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter ~~(p, q, pinv, sp, dp, sq, dq)~~ by corrupting at least one first key parameter (Walmsley page 12, paragraphs 0301-0303 and 0312) ~~(p, q, pinv, sp, dp, sq, dq), characterized in that at least one key parameter (dp, dq) is the product of a value required for the cryptographic calculation times a safeguard value (sp, sq), and in that the integrity check (30, 34, 40, 54) includes a divisibility check~~.

As to claim 14, Walmsley discloses a method as claimed in claim 1, wherein in the integrity check it is determined whether the value of at least one key parameter is contained in a range of valid values, wherein the range is non-contiguous in that it has a plurality of gaps (Walmsley page 40, paragraph 0998).

As to claim 15, Walmsley discloses a method as claimed in claim 1, wherein in the integrity check it is determined whether at least two key parameters are in a predetermined relationship to one another (Walmsley page 40, paragraph 0998: internally generating $S[K_1|K_2]$ and comparing against Checksum).

As to claim 19, Walmsley discloses a method as claimed in claim 1, wherein in the integrity check a checksum stored with the key parameters is compared with a checksum newly

calculated after passing of the key parameters (Walmsley page 13, paragraphs 0036-034 and page 14, paragraphs 0036).

As to claim 20, Walmsley discloses a method as claimed in claim 1, wherein, to check the integrity, important parameters to be passed are multiply passed and checked for identity after passing (Walmsley page 13, paragraphs 0036-034 and page 14, paragraphs 0036).

As to claim 27, Walmsley discloses a method for determining a key for a cryptographic calculation with at least two key parameters, the key being adapted to be used in a method for protected execution of a cryptographic calculation wherein an integrity check of the key is performed (Walmsley page 36, paragraphs 0933-0945, page 14, paragraphs 0352-0354) in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter (Walmsley page 12, paragraphs 0301-0303 and 0312).

As to claim 30, Walmsley discloses a computer program product which has program commands to cause a processor to execute a method (Walmsley page 14, paragraph 0058) for protected execution of a cryptographic calculation, in which a key with at least two key parameters is drawn on, wherein an integrity check of the key is performed (Walmsley page 36, paragraphs 0933-0945, page 14, paragraphs 0352-0354) in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter (Walmsley page 12, paragraphs 0301-0303 and 0312).

As to claim 32, Walmsley discloses a portable data carrier set up for executing a method (Walmsley page 4, paragraph 0097) for protected execution of a cryptographic calculation, in which a key with at least two key parameters is drawn on, wherein an integrity check of the key

is performed (Walmsley page 36, paragraphs 0933-0945, page 14, paragraphs 0352-0354) in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter (Walmsley page 12, paragraphs 0301-0303 and 0312).

As to claim 33, Walmsley discloses a portable data carrier as claimed in claim 32, wherein the data carrier is one of a smart card and a chip module (Walmsley page 4, paragraph 0097).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 16-18, 21-26, 28, 29, 31, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over WO 0161918 (US 20030159036) (Walmsley) (Applicant's IDS) in view of US 20030097628 (Ngo) and in view of US 6965673 (Boneh).**

As to claim 16, Walmsley discloses a method as claimed in claim 1. Walmsley fails to teach wherein the integrity check includes a multiplicative operation, in particular a divisibility test.

However, Ngo discloses wherein the integrity check includes a multiplicative operation, in particular a divisibility test (Ngo page 1, paragraph 0009).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because to use a divisibility test for an integrity check is a cheaper and a faster calculation (Ngo page 1, paragraph 0009).

As to claim 17, Walmsley discloses a method as claimed in claim 1. Walmsley fails to teach wherein in the integrity check it is checked whether at least one of the key parameters is evenly divisible by the safeguard value.

However, Ngo discloses wherein in the integrity check it is checked whether at least one of the key parameters is evenly divisible by the safeguard value (Ngo page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because again the divisibility check is cheaper and faster as well as if you use a predetermined value it adds to the assurance that there are no errors or whether or not corruption has occurred (Ngo page 2, paragraph 0026).

As to claim 18, Walmsley discloses a method as claimed in claim 1. Walmsley fails to teach wherein in the integrity check it is checked whether at least one value which differs from one of the key parameters by a multiple of a safeguard value is evenly divisible by the safeguard value.

However, Ngo discloses wherein in the integrity check it is checked whether at least one value which differs from one of the key parameters by a multiple of a safeguard value is evenly divisible by the safeguard value (Ngo page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because to add another multiple as a blinding factor increases the security of the protected calculation (Ngo page 2, paragraph 0026).

As to claim 21, Walmsley discloses a method as claimed in claim 1. Walmsley fails to teach wherein the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA method.

However, Boneh discloses wherein the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA method (Boneh column 7, lines 30-37).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Boneh because RSA decryption and signature generation are well know cryptographic calculations and to use these protected calculations would increase there security (Boneh column 7, lines 30-37).

As to claim 22, the modified Walmsley discloses a method as claimed in claim 21. The modified Walmsley fails to teach wherein the RSA method is an RSA-CRT method.

However, Boneh discloses wherein the RSA method is an RSA-CRT method (Boneh column 7, lines 20-65).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Boneh because the RSA-CRT is a well know cryptographic calculation and to use these protected calculations would increase there security (Boneh column 7, lines 20-65).

As to claim 23, the modified Walmsley discloses a method as claimed in claim 21. The modified Walmsley fails to teach wherein in the cryptographic calculation at least one exponentiation operation is performed and in the integrity check it is checked whether the exponent used in the exponentiation operation is evenly divisible by a safeguard value.

However, Ngo discloses wherein in the cryptographic calculation at least one exponentiation operation is performed and in the integrity check it is checked whether the exponent used in the exponentiation operation is evenly divisible by a safeguard value (Ngo page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because the divisibility check is cheaper and faster as well as if you use a predetermined value it adds to the assurance that there are no errors or whether or not corruption has occurred (Ngo page 2, paragraph 0026).

As to claim 24, the modified Walmsley discloses a method as claimed in claim 23. The modified Walmsley fails to teach wherein in the cryptographic calculation an exponent blinding method is applied for protection against spying.

However, Boneh discloses wherein in the cryptographic calculation an exponent blinding method is applied for protection against spying (Boneh column 17, lines 41-46).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Boneh because to add another multiple as a blinding factor increases the security of the protected calculation (Boneh column 17, lines 41-46).

As to claim 25, the modified Walmsley discloses a method as claimed in claim 21, wherein the prime factors of the RSA method are multiplied by a masking parameter and the error freedom of the calculation sequence is checked by an equality check modulo the masking parameter (Walmsley page 4, paragraph 0089).

As to claim 26, Walmsley discloses a method as claimed in claim 1. Walmsley fails to teach wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.

However, Ngo discloses wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check (Ngo page 1, paragraph 0009 and page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because the divisibility check is cheaper and faster as well as if you use a predetermined value it adds to the assurance that there are no errors or whether or not corruption has occurred and to add another multiple as a blinding factor increases the security of the protected calculation (Ngo page 1, paragraph 0009 and page 2, paragraph 0026).

As to claim 28, Walmsley discloses a method as claimed in claim 27. Walmsley fails to teach characterized in that at least one key parameter is obtained by multiplication of a value required for the cryptographic calculation by a safeguard value.

However, Ngo discloses characterized in that at least one key parameter is obtained by multiplication of a value required for the cryptographic calculation by a safeguard value (Ngo page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because to add another multiple as a blinding factor increases the security of the protected calculation (Ngo page 2, paragraph 0026).

As to claim 29, Walmsley discloses a method as claimed in claim 27. Walmsley fails to teach wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.

However, Ngo discloses wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check (Ngo page 1, paragraph 0009 and page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because the divisibility check is cheaper and faster as well as if you use a predetermined value it adds to the assurance that there are no errors or whether or not corruption has occurred and to add another multiple as a blinding factor increases the security of the protected calculation (Ngo page 1, paragraph 0009 and page 2, paragraph 0026).

As to claim 31, Walmsley discloses a computer program product as claimed in claim 30. Walmsley fails to teach wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.

However, Ngo discloses wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check (Ngo page 1, paragraph 0009 and page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because the divisibility check is cheaper and faster as well as if you use a predetermined value it adds to the assurance that there are no errors or

whether or not corruption has occurred and to add another multiple as a blinding factor increases the security of the protected calculation (Ngo page 1, paragraph 0009 and page 2, paragraph 0026).

As to claim 34, Walmsley discloses a portable data carrier as claimed in claim 32. Walmsley fails to teach wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.

However, Ngo discloses wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check (Ngo page 1, paragraph 0009 and page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because the divisibility check is cheaper and faster as well as if you use a predetermined value it adds to the assurance that there are no errors or whether or not corruption has occurred and to add another multiple as a blinding factor increases the security of the protected calculation (Ngo page 1, paragraph 0009 and page 2, paragraph 0026).

Prior Art

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 5390196 is pertinent because it teaches…A binary polynomial is a polynomial in which all coefficients are either one or zero. A CRC is generated by dividing data to be validated by a predetermined binary polynomial prior to storage or transmission. The remainder from the

division operation is the CRC or "checksum", and this code is usually appended to the data to be validated. For validation, the data with the appended CRC is divided again by the same polynomial. If the data is unchanged, a zero remainder will result. Anything other than a zero remainder indicates that the data has been corrupted. US 5799086 is pertinent because it teaches… A cryptographic system with key escrow feature that uses a method for verifiably splitting user's private encryption keys into components and for sending those components to trusted agents chosen by the particular users is provided. The system uses public key certificate management, enforced by a chip device that also self-certifies. The methods for key escrow and receiving an escrow certificate are applied to register a trusted device with a trusted third party and to receive authorization from that party enabling the device to communicate with other trusted devices. The methods for key escrow also provide assurance that a trusted device will engage in electronic transactions in accordance with predetermined rules. US 5991415 is pertinent because it teaches… Improved methods and apparatus are provided for protecting public key schemes based on modular exponentiation (including RSA and Diffie-Hellman) from indirect cryptanalytic techniques such as timing and fault attacks. Known methods for making the implementation of number-theoretic schemes resistant to such attacks typically double their running time, whereas the novel methods and apparatus described in this patent add only negligible overhead. This improvement is particularly significant in smart card and software-based implementations, in which the modular exponentiation operation is quite slow, and doubling its time may be an unacceptable solution. US 6052469 is pertinent because it teaches… A cryptographic key recovery system that is interoperable with existing systems for establishing keys between communicating parties. The sender uses a reversible key inversion function to

generate key recovery values P, Q and (optionally) R as a function of a session key and public information, so that the session key may be regenerated from the key recovery values P, Q and (if generated) R. Key recovery values P and Q are encrypted using the respective public recovery keys of a pair of key recovery agents. The encrypted P and Q values are included along with other recovery information in a session header accompanying an encrypted message sent from the sender to the receiver. The key recovery agents may recover the P and Q values for a law enforcement agent by decrypting the encrypted P and Q values in the session header, using their respective private recovery keys corresponding to the public keys. The R value, if generated, is not made available to the key recovery agents, but is ascertained using standard cryptanalytic techniques in order to provide a nontrivial work factor for law enforcement agents. The receiver checks the session header of a received message to ensure that the sender has included valid recovery information. Only when the receiver has verified that the sender has included valid recovery information does the receiver decrypt the received message. US 20030061498 is pertinent because it teaches… According to the invention the data storage medium is designed in order to split secret data, which is stored in the semiconductor chip in order to carry out security-relevant or safety-relevant operations or is generated by this semiconductor chip, into at least three data parts, with an arithmetic unit being included in order to calculate a random number and in order to divide the random number, with the first data part being the integer result of the division process, the second part being the remainder of the division process, and the third part being the random number itself. US 20050084096 is pertinent because it teaches… The invention concerns a method for implementing in an electronic component a cryptographic algorithm using calculating means. The invention is characterized in that it consists in carrying

out the following steps: a) selecting a value e among a specific number of values e.sub.1, e.sub.i being integers, b) checking if e.sub.i verifies a predetermined relationship: if so, then e=e.sub.i, and storing e for use in calculating said cryptographic algorithm. US 6914983 is pertinent because it teaches… The modular exponentiation function used in public key encryption and decryption systems is implemented in a standalone engine having at its core modular multiplication circuits which operate in two phases which share overlapping hardware structures. The partitioning of large arrays in the hardware structure, for multiplication and addition, into smaller structures results in a multiplier design comprising a series of nearly identical processing elements linked together in a chained fashion. As a result of the two-phase operation and the chaining together of partitioned processing elements, the overall structure is operable in a pipelined fashion to improve throughput and speed. The chained processing elements are constructed so as to provide a partitionable chain with separate parts for processing factors of the modulus. In this mode, the system is particularly useful for exploiting characteristics of the Chinese Remainder Theorem to perform rapid exponentiation operations. A checksum mechanism is also provided to insure accurate operation without impacting speed and without significantly increasing complexity. While the present disclosure is directed to a complex system which includes a number of features, the present application is particularly directed a system and method for performing modular checksum operations. US 7227947 is pertinent because it teaches… The invention relates to a cryptographic method with at least one computing step containing a modular exponentiation E according to E=x.sup.d(mod pq), with a first prime factor p, a second prime factor q, an exponent d and a number x, whereby the modular exponentiation E is calculated according to the Chinese Remainder Theorem.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Rebecca L. Pachura whose telephone number is (571) 270-3402. The examiner can normally be reached on Monday-Thursday 7:30 am-6:00 pm est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Rebecca L Pachura/
Examiner, Art Unit 2136

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136